ISRCS 2011

Towards Resilient Critical Infrastructures: Application of Type-2 Fuzzy Logic in Embedded Network Security Cyber Sensor

Ondrej Linda, Todd Vollmer, Milos Manic, Jim Alves-Foss

Date: 8/9/2011

University of Idaho
Idaho Falls

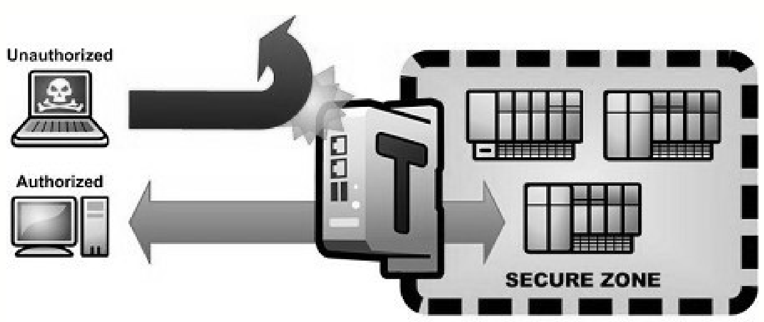
Idaho National Laboratory

Presentation Outline

- Overview of Previous Work and Fuzzy Logic
- Embedded Network Security Cyber Sensor
- Online Learning Algorithm for Anomaly Detection
- Experimental Results
- Conclusion

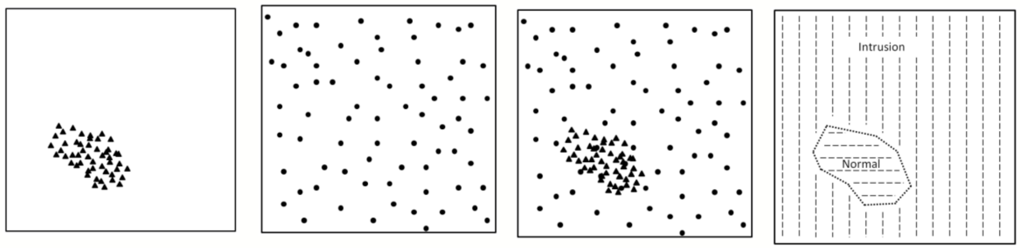
Cyber-Security of Critical Infrastructures

- Protection against cyber attacks and cyber terrorism
- Critical infrastructures (e.g. nuclear power plants, SCADA) are vulnerable
- Development of System Protection Cyber Sensor
  - Easy to deploy
  - Low Cost
  - Increased State-Awareness



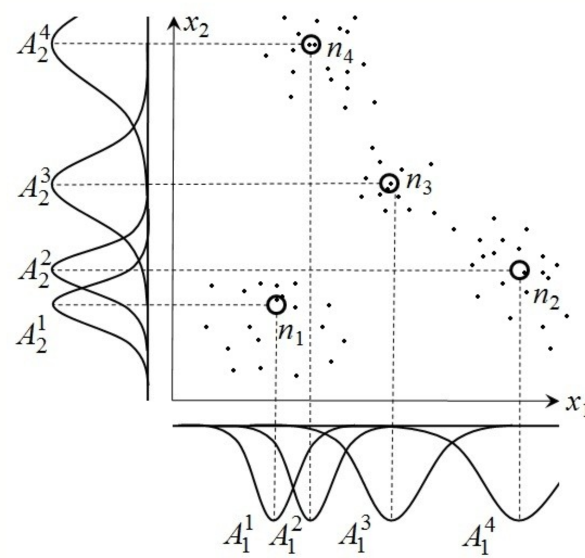
Previous Work

- Neural Network Based Intrusion Detection System for Critical Infrastructures
  - offline training, not suitable for embedded cyber sensor



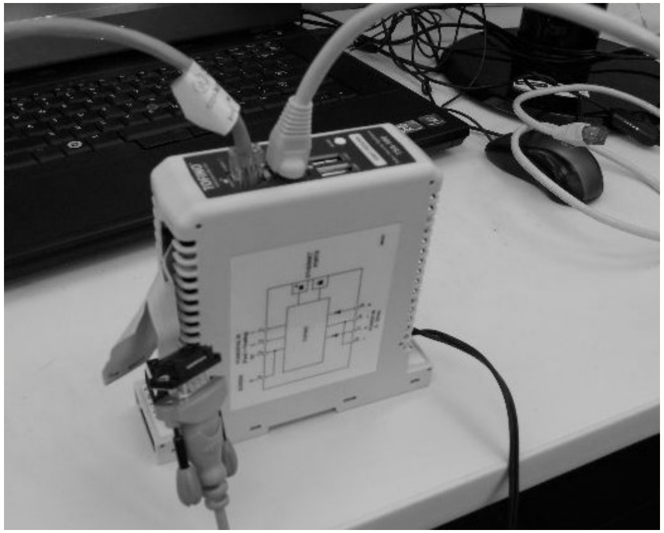
Normal Behavior | Simulated Intrusions | Combined | ANN Classification

- Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor
  - Automatic fuzzy rule construction using one-pass online clustering algorithm
  - Suitable for constrained computational resources of embedded devices



Current Work

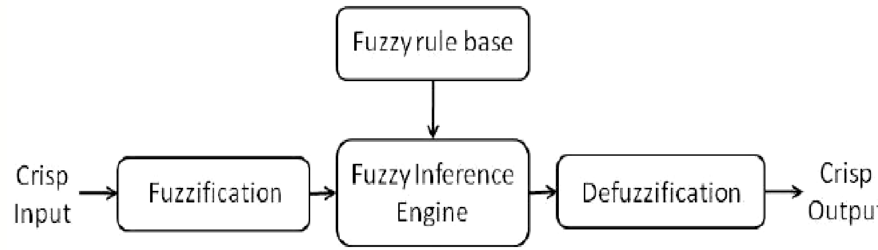
- Extending the previous work
  - Using Interval Type-2 Fuzzy Logic for robust anomaly detection and increased cyber-security state awareness.
  - Computationally efficient algorithm for the low-cost embedded network security cyber sensor



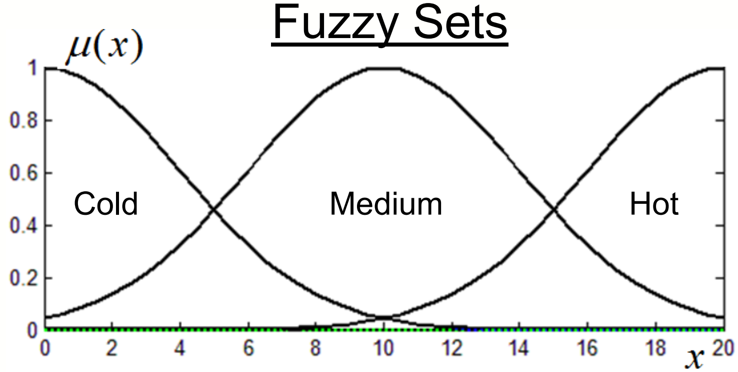
Type-1 Fuzzy Logic Controller (FLC)

- T1 FLC
  - Set of linguistic rules
  - Fuzzy sets describe ambiguous, imprecise words

T1 Fuzzy Logic System



Fuzzy Sets



Rule Firing Strength (minimum t-norm)

$$\mu_{R_k}(\vec{x}) = \min_{i=1..n}\{\mu_{A_i^k}(x_i)\}$$

Fuzzy Linguistic Rules

Rule R_k: **IF** x_1 is A_1^k **AND** … **AND** x_n is A_n^k **THEN** y_k is B^k

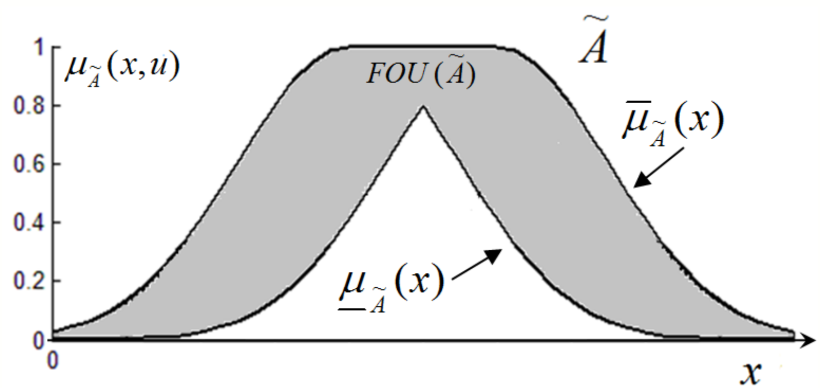
Defuzzification (centroid defuzzifier)

$$y = \frac{\sum_{i=1}^{N} y_i \mu_B(y_i)}{\sum_{i=1}^{N} \mu_B(y_i)}$$

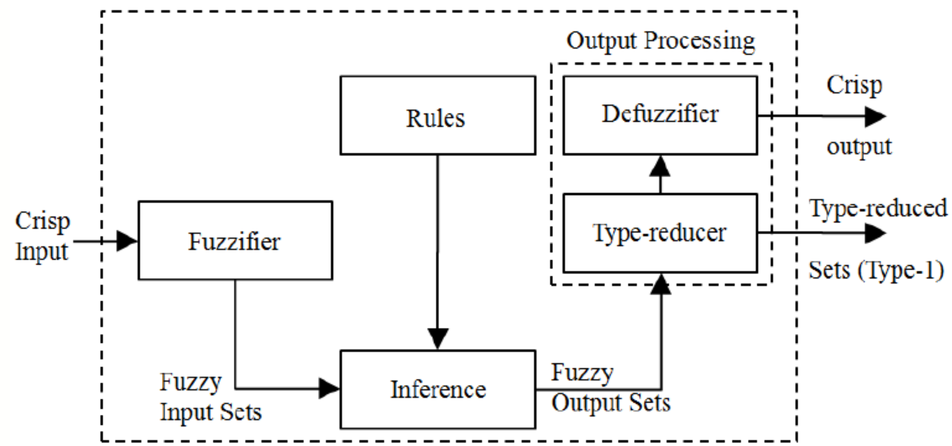
Interval Type-2 FLC

- T1 FLC performance is susceptible to dynamic uncertainty
- IT2 FLC provides better handling of dynamic uncertainties
  - Implements additional dimension of uncertainty – secondary grade
  - Interval T2 fuzzy sets are described by footprint of uncertainty – FOU
  - FOU is bounded by upper and lower membership function

$$FOU(\tilde{A}) = \bigcup_{\forall x \in X} (\underline{\mu}_{\tilde{A}}(x), \bar{\mu}_{\tilde{A}}(x))$$



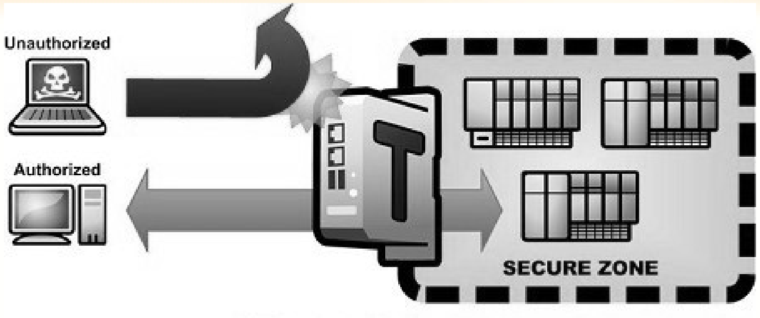
T2 Fuzzy Logic System



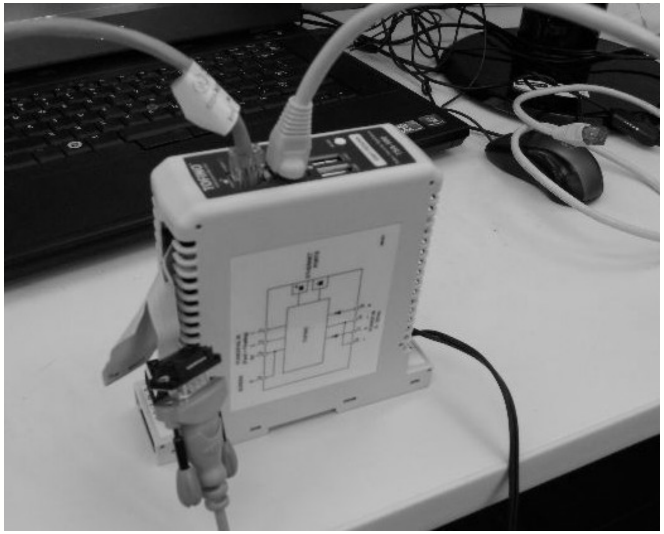
Cyber-Sensor

- Embedded Network Security

  Cyber Sensor



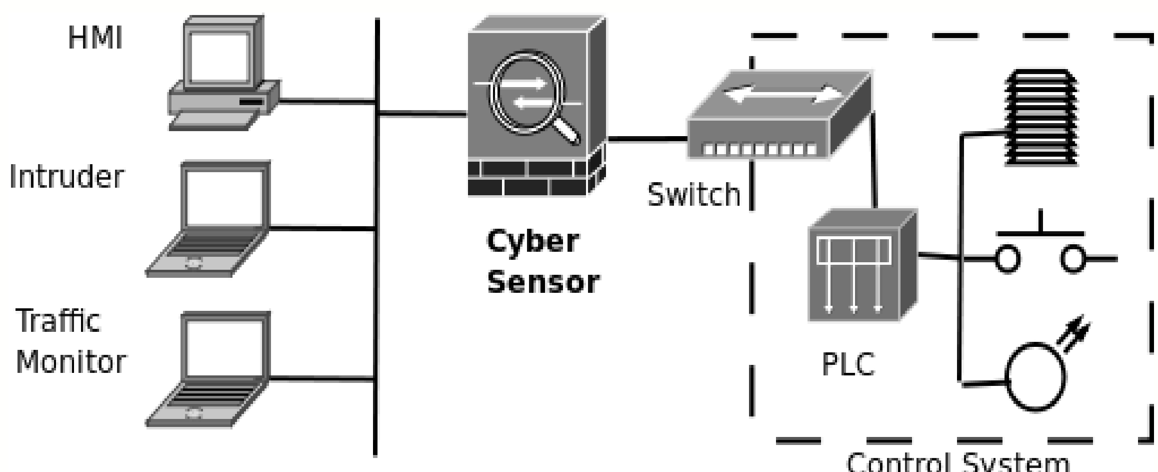
- Deployment at low level before the critical component (e.g. PLC)
  - Requirements of low cost.



- Tofino embedded network security device
  - Manufactured by Byres Security Inc.
  - Pre-emptive threat detection, termination and reporting
  - Specifically tailored for the needs of SCADA and industrial control systems
  - Intel IXP425 processor, 533MHz, 64MB DRAM

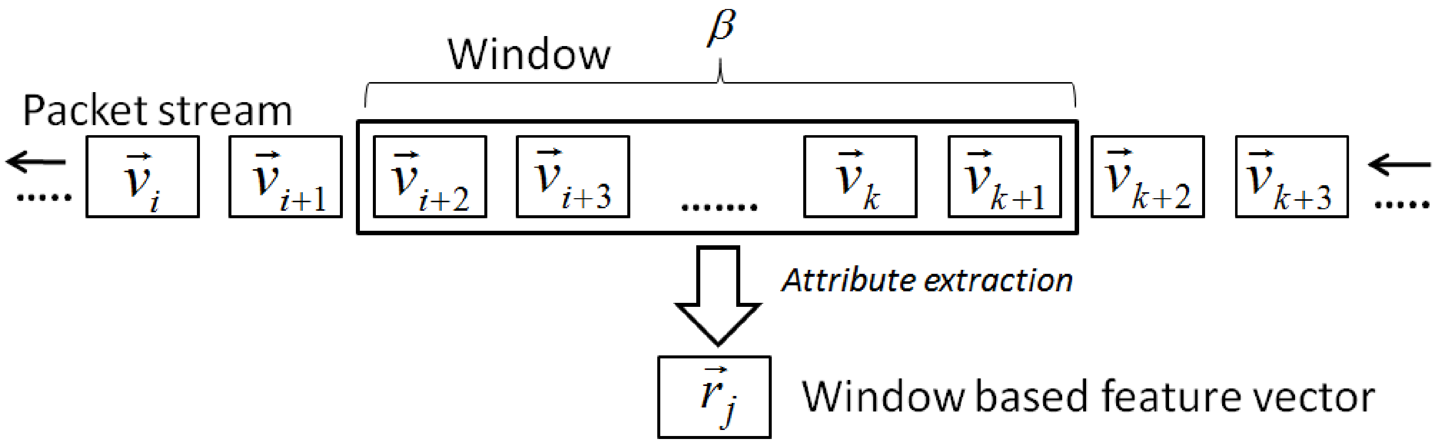
Network Data Acquisition

- Experimental test-bed
  - Represents various aspects of operational control structure
  - RSView32 integrated component monitoring interface
  - Allen-Bradley MicroLogix 1100 PLC
  - Sub-systems with buttons, potential meters fans, lights
  - Linux laptop with *tcpdump* software for network traffic capturing and monitoring
  - Experimental data contains normal behavior and simulated intrusion attempts



Network Data Preprocessing

- Uses sliding window to compute statistical properties of a sequence of packets:



- Examples of extracted attributes: # IPs, Avg. time, # Protocols, # Flag Codes, # 0 Win. Size, # 0 Data Len., Avg. Win. Size, Avg. Data Len.

Online Learning Algorithm

- Low-memory and computational time requirements
- Based on one-pass nearest neighbor clustering

Input:

$$X = \{\vec{x}_1, \ldots, \vec{x}_N\},\ \vec{x}_i \in \Re^n$$

Output: Set of Clusters

$$P_i = \{\vec{c}_i, w_i\},\ \vec{c}_i \in \Re^n, w_i \in \aleph^+$$

- 1) Initialize cluster P_1 at position of pattern $\vec{x}_1$
- 2) Iterate through all patterns and find the nearest cluster:

$$dist(\vec{c}_a, \vec{x}_i) = \min_j \sqrt{\left(c_j^1 - x_i^1\right)^2 + \ldots + \left(c_j^n - x_i^n\right)^2},\ j = 1 \ldots C$$

- 3) If $dist(\vec{c}_a, \vec{x}_i) \le rad$ then add pattern $\vec{x}_i$ to cluster P_a

$$\vec{c}_a = \frac{w_a \vec{c}_a + \vec{x}_i}{w_a + 1},\ w_a = w_a + 1$$

Else, create new cluster at position of pattern $\vec{x}_i$

Online Learning Algorithm

- Online network behavior patterns extraction
  - Apply the Nearest Neighbor clustering to the incoming pre-processed stream of packets
  - Also accumulate statistical information about the patterns assigned to each cluster

- Cluster attributes:

$$P_i = \{\vec{c}_i, w_i, M_i\},\ \vec{c}_i = \{c_i^1, \ldots, c_i^n\},\ M_i = \begin{vmatrix} c_{i,1}^U & \cdots & c_{i,n}^U \\ c_{i,1}^L & \cdots & c_{i,n}^L \end{vmatrix}$$

- Modified cluster update rule for the Nearest Neighbor clustering:

$$\vec{c}_a = \frac{w_a \vec{c}_a + \vec{x}_i}{w_a + 1},\ w_a = w_a + 1$$

$$\overline{c}_i^j = \max(x_i^j, \overline{c}_i^j),\ \underline{c}_i^j = \min(x_i^j, \underline{c}_i^j) \quad j = 1 \ldots n$$

IT2 Fuzzy Rules Extraction

- During the testing phase, individual clusters are used to initialize IT2 fuzzy rules:

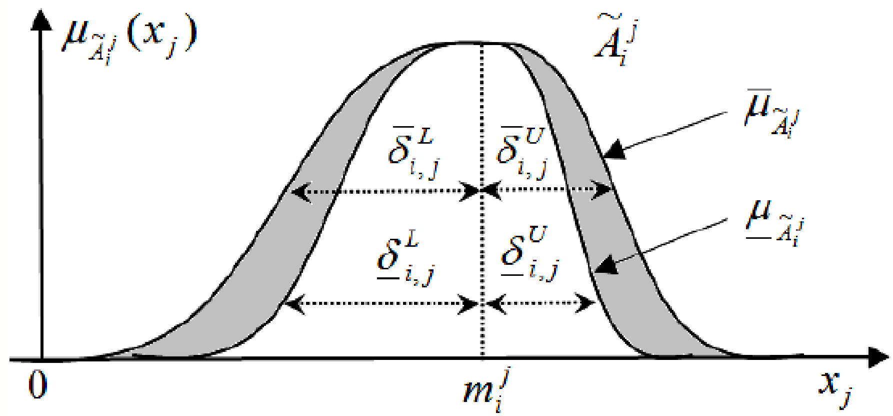
$$\text{Rule } R_k\text{: } \mathbf{IF}\ x_1 \text{ is } \widetilde{A}_1^k\ \mathbf{AND} \ldots \mathbf{AND}\ x_n \text{ is } \widetilde{A}_n^k\ \mathbf{THEN}\ y_k \text{ is } \widetilde{B}^k$$

- Non-symmetric Gaussian IT2 fuzzy set:
  - Uses an interval fuzziness parameter $[\underline{\alpha}, \overline{\alpha}]$

$$m_{i,j} = c_{i,j}$$

$$[\underline{\delta}^U_{i,j}, \overline{\delta}^U_{i,j}] = \left[\underline{\alpha}(c^U_{i,j} - c_{i,j}), \overline{\alpha}(c^U_{i,j} - c_{i,j})\right]$$

$$[\underline{\delta}^L_{i,j}, \overline{\delta}^L_{i,j}] = \left[\underline{\alpha}(c_{i,j} - c^L_{i,j}), \overline{\alpha}(c_{i,j} - c^L_{i,j})\right]$$



  - Rules describe the similarity of the observed behavior and the normal behavior. Hence, the output of each rule is its own firing strength

IT2 Fuzzy Rule Based Anomaly Detection

- Uses IT2 fuzzy logic inference with the extracted set of normal network behavior fuzzy rules:

  Rule R_k: **IF** x_1 is $\widetilde{A}_1^k$ **AND** … **AND** x_n is $\widetilde{A}_n^k$ **THEN** y_k is $\widetilde{B}^k$

- Degree of Firing: $\underline{\mu}_{R_i}(\vec{x}) = \min_{j=1..n}\{\underline{\mu}_{\widetilde{A}_i^j}(x_j)\}$ $\overline{\mu}_{R_i}(\vec{x}) = \min_{j=1..n}\{\overline{\mu}_{\widetilde{A}_i^j}(x_j)\}$

- Aggregate rule outputs: $\underline{y}(\vec{x}) = \max_{i=1..C}\underline{\mu}_{R_i}(\vec{x})$ $\overline{y}(\vec{x}) = \max_{i=1..C}\overline{\mu}_{R_i}(\vec{x})$

- Defuzzified Output: $$y = \frac{(\underline{y}(\vec{x}) + \overline{y}(\vec{x}))}{2}$$

- Output Decision:

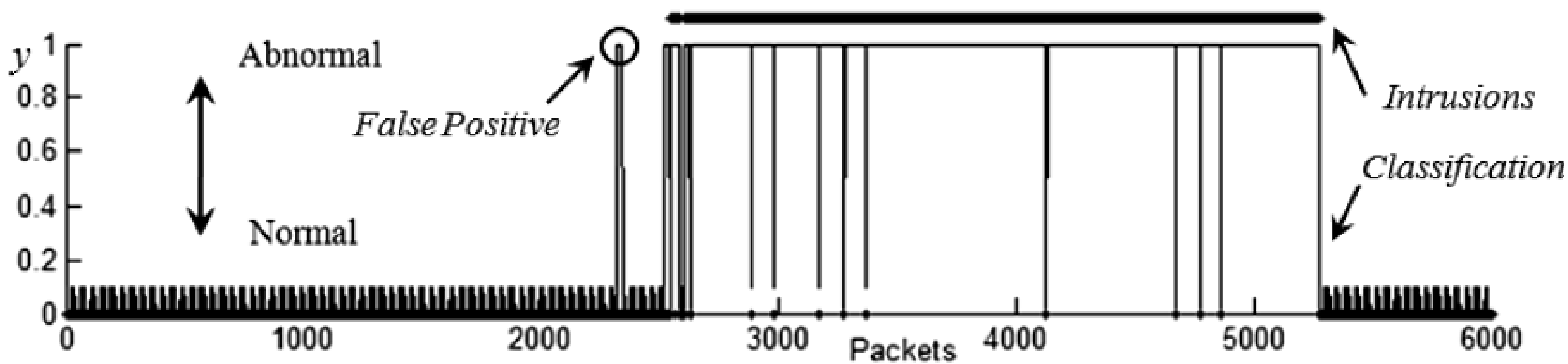
  If $\underline{y}(\vec{x}) >$ threshold **Then** Anomaly behavior.

  Else If $\overline{y}(\vec{x}) <$ threshold **Then** Normal behavior.

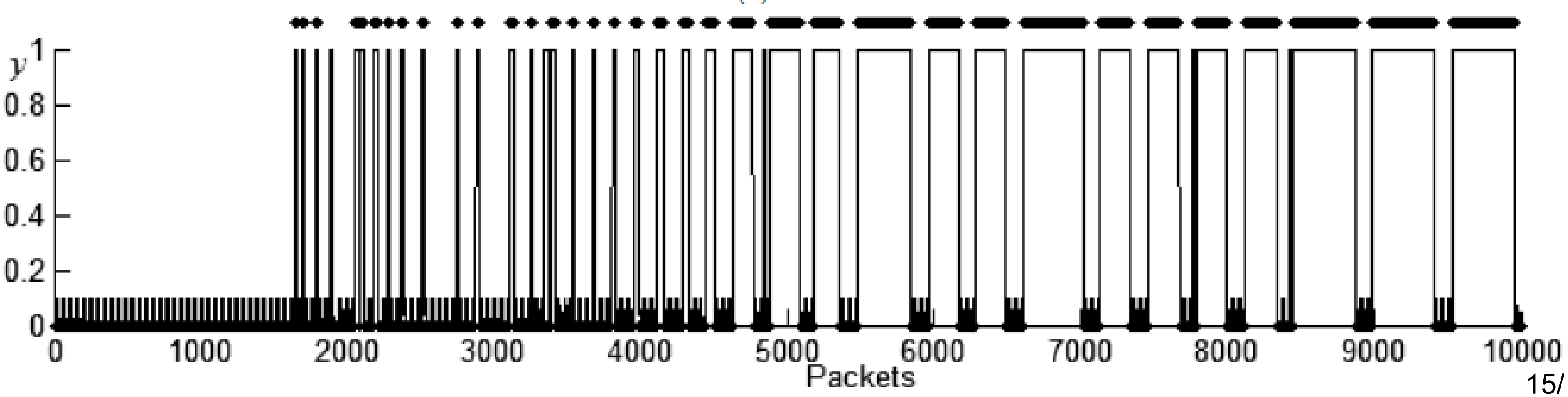
  Else If $\underline{y}(\vec{x}) <$ threshold $< \overline{y}(\vec{x})$ **Then** Uncertain behavior.

Experimental Results

- Training data – 6 datasets with 60,661 packets of normal behavior
- Testing data – 10 datasets with 583,637 packets of abnormal behavior



(a)



Experimental Results

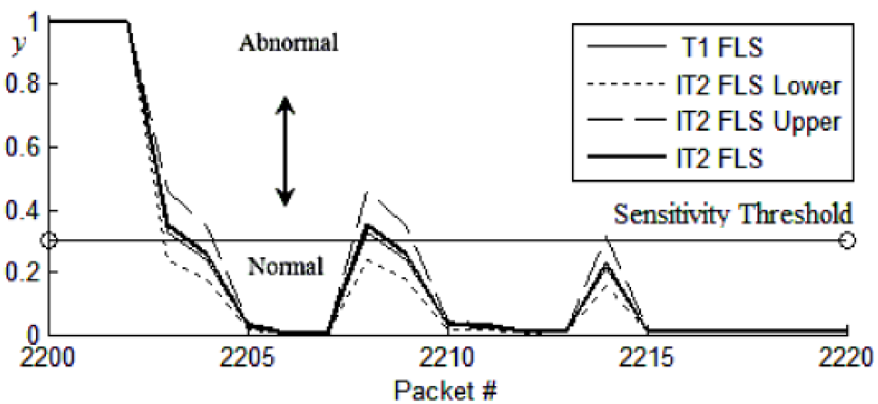
- 132 fuzzy rules generated
- 0% false negative rate and 1.3% false positive rate

Datasets	Number of Packets	Classification Rate	False Positives
Data 1	16,860	99.226 %	0.857%
Data 2	11,794	99.276 %	0.840 %
Data 3	21,904	99.327 %	0.727 %
Data 4	18,225	99.321 %	0.809 %
Data 5	34,586	99.385 %	1.372 %
Data 6	113,705	98.277 %	1.772 %
Data 7	113,557	98.339 %	1.804 %
Data 8	65,018	98.438 %	1.606 %
Data 9	69,959	98.521 %	1.519 %
Data 10	118,029	98.259 %	1.791 %
Sum / Average	583,637	98.837 %	1.310 %

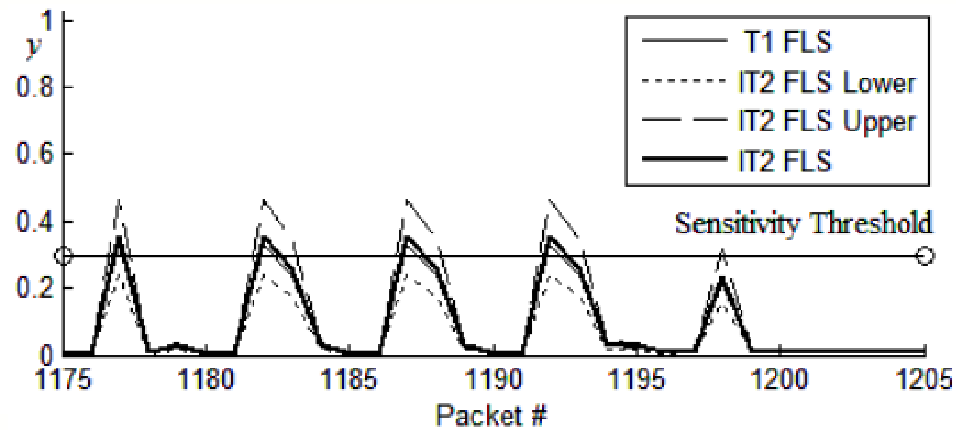
Experimental Results

- Improved Uncertainty handling

Similar intrusion attempt



Unusual normal behavior



Conclusion

- Developed an IT2 FLS based anomaly detection algorithm for embedded network security cyber sensor.

- The algorithm extracts IT2 fuzzy rules using an adapted version of the online nearest neighbor clustering algorithm directly from the stream of packets.

- The IT2 FLS offers improved cyber-security state awareness due to improved uncertainty handling by IT2 FSs.

Acknowledgement

- This work was supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DE-AC07-05ID14517, performed as part of the Instrumentation, Control, and Intelligent Systems Distinctive Signature (ICIS) of Idaho National Laboratory.